



Government
eProcurement
System

eProcurement System Government of India

Published Corrigendum Details

Date : 22-Oct-2025 11:40 AM

Print

Organisation Chain :	Director-Indian Institute of Technology(IIT Delhi) Dy.Registrar(Stores) Central Store Purchase Section-IIT Delhi
Tender ID :	2025_IIT_881811_1
Tender Ref No :	FT/NCIIPC/RFP/2025-2026
Tender Title :	Design, Build, Installation, Testing Commissioning, Integration, and Operations and Maintenance of IT Infrastructure for AI Grand challenge at NCIIPC Datacenter and incubation center at Ayanagar, New Delhi.
Corrigendum Type :	Technical Bid

Corrigendum Document Details					
Corr.No.	Corrigendum Title	Corrigendum Description	Published Date	Document Name	Doc Size(in KB)
1	Firewall Technical Specifical	We have erroneously published the worn specifications for the firewall. Please use the below given specifications for both the firewall pairs. Rest there are no changes in any other clauses in the RFP	22-Oct-2025 11:39 AM	Firewall_Specs.pdf 	601.01

Refer Part B TECHNICAL SPECIFICATION HARDWARE, PROJECT GOVERNANCE and SECURITY Para 2.4.5 Common features(Technical specification) .

We have erroneously published the worn specifications for the firewall. Please use the below given specifications for both the firewall pairs. Rest there are no changes in any other clauses in the RFP

2.4.5 Firewalls

2.4.5.1 Perimeter (Internet LAN): Secure Firewall HA pair with URL filtering, IPS, DNS security

2.4.5.2 ISFW (Internal Segmentation): Secure Firewall HA pair sized for east-west inter-VRF traffic; IPS enabled on allowed flows; no NAT

S/N	Specification	Compliance (Yes/No)
1	The Firewall appliance must be non-ASIC based and should have Multi core architecture to mitigate against the sophisticated threats. If option to disable ASIC is there, then OEM must mention the performance numbers in datasheet (without ASIC)	
2	The Firewall appliance must have a hardened operating system from the OEM and should have 8 Core CPU with 32 GB of RAM to make sure all the security capabilities are provided without degradation from day one.	
3	The Firewall appliance must have minimum 8x10G and 8x1G Ports from day 1 with required SR transceivers as per the ports. Also should have atleast 1 additional network I/O slot to add 8*10G or 2x40G or 4*25G ports in future, depending upon organization's choice. If future choice is not possible then all ports to be provided from day1.	
4	The Firewall appliance should not be more than 1U rack- mounted design and must have redundant field replaceable/ hot swappable power supply to remove any single point of failure.	
5	The Firewall appliance must deliver 10 Gbps NGFW throughput with Security features (FW, IPS, and Application Control) enabled and 9 Gbps Threat Prevention throughput. The same must be available in the public datasheet. (must submit evidence)	
6	The Firewall appliance must deliver 35 Gbps of IPSEC VPN throughput from day 1 and should support 80K concurrent IPsec VPN SAs without any limitation of VPN Clients.	
7	The Firewall appliance must deliver minimum 2.5 Gbps of TLS/SSL inspection throughput and 650K concurrent inspected HTTP connections from day1 as default value without adding any additional license.	
8	The Firewall appliance must deliver 500K new connections/sessions per sec and 30 million concurrent connections/sessions from day1 and these should be available per appliance as default no's without additional license.	
9	The Firewall appliance must have the security features including IPS, Application Awareness, Anti-Bot, DOS prevention, URL filtering, Anti-	

	Malware, AETs including routing features to be managed from the Central console, no need for any configuration via appliance GUI and Appliance CLI. Solution also support integration with Snort.	
10	The solution must use the server name indication for the https traffic for URL categorization without decrypting the https connection	
11	Solution must support client based agent to check the security posture of endpoints and must be able to employ policies basis the attributes. Policy must be defined on NGFW for discarding the user requests if AV is not updated, OS version is Obsolete, Load on Endpoint is high / any users is using the obsolete browsers and should not have any dependencies on the number of client supported & there is should not be any license attached to it.	
12	Solution must have support TLS 1.3 and TLS/SSL server certificate verification before decryption decision is taken and must support full-stream reconstruction with high- speed exploit fingerprinting to examines actual payloads along with connection, usage, command controls	
13	Solution must prevent against the websites via URL filtering that mask their identity using Dynamic DNS services, Elevated exposure by website that camouflage their true nature, domain name that are registered recently, parked domain, Unauthorized Mobile Marketplaces to prevent users visiting the websites that may distribute applications unauthorized by the mobile OS manufacture	
14	Solution must be able to prevent the users to visit the websites that use technologies that alter the operation of a user's hardware, software, or network to decrease owner's control with the intent to gain fraudulent access and with potential malicious intent.	
15	Solution must be able to prevent the users to visit the websites that enable download of software applications or file download servers, download of media content, client software to enable peer-to-peer file sharing and transfer, Sites that store personal files on web servers for backup or exchange.	
16	Solution should support Re-authentication when using browser-based user authentication and support 4096 bit RSA key for Browser Based User Authentication.	
17	Solution should support local user creation options via Central Manager and also support the use of external CA issued certificates in internal management communication and Centralized manager should support to block the access temporarily after multiple failed logon attempts from the same IP.	
18	Solution must have enhanced engine monitoring capability and support for non-TCP traffic, applications that use UDP for data transport.	
19	Solution must have the following categories to take action and to use them in the access rule like abused Drugs, adult content & material, alcohol & tobacco, gambling, hacking, Illegal or Questionable, Intolerance, Marijuana, Militancy & Extremist, Nudity, Sex, Advanced Malware, Bot Networks, Compromised Websites, Custom Encrypted Uploads, Malicious Web Sites, Mobile Malware, Phishing and other Frauds, Potentially Exploited Documents, Proxy Avoidance, P2P, Personal Network Storage, Streaming media, spyware, etc	
20	Solution must be able to detect protocol abnormality & misuse detection with Exploit and malware detection via high-speed DFA.	

21	The Firewall appliance must support L3 protocol functionality like Static & policy-based routing, static multicast routing, dynamic routing like MP-BGP, RIPng, OSPF(v2 & v3), IGMP proxy, BGP, BFD, PIM (SM & SSM), and Application-aware routing.	
22	The Firewall solution must support IPv4 and IPv6 from day one. Solution should support NAT66, NAT64, NAT44, and PAT from day 1 and must support Stateless IPv4/IPv6 translation.	
23	The Firewall appliance must support IPv6 capability including Dual stack IPv4/IPv6, ICMPv6, DNSv6, IPv6 static, SLAAC, DHCPv6 relay.	
24	The Firewall appliance must support TLS 1.3 and TLS/SSL server certificate verification before decryption decision is taken.	
25	The Firewall appliance must support security proxies for the following TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS.	
26	The Firewall appliance must have Firewall for stateful blocking, URL filtering, Anti-Spoofing, IP Reputation, Geo- Protection, Dropping Invalid Connections.	
27	The Solution must allow the administrator to configure CRLs to be fetched and cached even before those are needed for certificate validation.	
28	The Solution must support SNMPv3 with support for SHA-256 and AES-256 algorithms.	
29	The Firewall solution must support L2 interfaces in the L3 deployment and must allow firewall with Layer 2 Interfaces using VXLAN to provides a solution for extending Layer 2 Interfaces across Layer 3 boundaries.	
30	The Firewall management system's web access interface should have an option to authenticate administrators by using client certificates.	
31	The solution must support client based agent to check the security posture of endpoints and must be able to employ policies basis the attributes. Policy must be defined on NGFW for discarding the user requests if AV is not updated, OS version is Obsolete, Load on Endpoint is high / any users is using the obsolete browsers.	
32	Solution must allow mixing of preshared keys as per the RFC 8784 in the IKEv2 to support post-quantum security.	
33	The solution must support high availability and load balancing between multiple ISPs, including VPN connections, Multi-Link VPN link aggregation, QoS-based link selection and admin should be able to manipulate the sensitivity of an application based on jitter, packet loss & latency.	
34	The solution must support configuration rollback feature to detect and recover from software and configuration errors by reverting back to previously active software or configuration.	
35	The Firewall appliance inspection engine must deliver more than 15000 fingerprint/vulnerabilities for detecting exploit attempts against known vulnerabilities in protocol specific tcp/udp port number. Solution must provide Multi-layer inspection to increase network security and performance and it should combine access control to define policies that govern your user's access to network resources, deep inspection to detect advanced threats & file filtering to block malicious file transfers.	
36	The solution must support 7000+ Applications for better control and visibility throughout the environment so that solution should be able to understand applications like 4sync, 4tube, bizible, facebook, youtube etc. Solution should support minimum of 10000 Inspection Signatures and should support QUIC & HTTP/3.	

37	The solution must support Full-Stream Deep Inspection, Anti-Evasion Defense, Dynamic Context Detection, Protocol-Specific Traffic Handling/Inspection, Granular Decryption of SSL/TLS Traffic, Vulnerability Exploit Detection, Custom Fingerprinting, Reconnaissance, Anti- Botnet, Correlation, Traffic Recording, DoS/DDoS Protection, Blocking Methods and Automatic Updates.	
38	The Firewall appliance Inspection Engine/ Anti-Bot must employ the below inspection technologies 1. Multilayer traffic normalization 2. Vulnerability-based fingerprints 3. Evasion and anomaly logging 4. Decryption-based detection 5. Message length sequence analysis	
39	The solution must support FTP and DNS Proxy to restrict the types of traffic and the commands that can be used with DNS and FTP connections. Solution must support DNS sink holing for UDP and TCP service.	
40	The solution must provide steering of applications dynamically & should provide application identification with link monitoring to effectively allocate networking resources, ensuring that the critical applications receive the necessary resources for optimal performance.	
41	The solution must have the technique for monitoring the application health and provide visibility into the organization's network traffic and the administrators should be able detect and resolve bottlenecks before they become a network-wide problem & should provide real- time visibility, historical views, and easy access to connectivity logs directly from the OEM Centralized management dashboard.	
42	The solution should have an option to create alternative policies if the connectivity between the NGFW and central Manager is lost, any policy should be allow to be selected whether it is a normal policy or one of the alternative policies	
43	The solution must prevent against the websites via URL filtering that mask their identity using Dynamic DNS services, Elevated exposure by website that camouflage their true nature, domain name that are registered recently, parked domain, Unauthorized Mobile Marketplaces to prevent users visiting the websites that may distribute applications unauthorized by the mobile OS manufacture	
44	The solution must have DNS sink holing for malicious DNS request from inside hosts to outside bad domains and blocks access to known malicious sites and non-existent IP addresses with ability to proactively measure against command and control (C2) access & second-stage malware downloads for disrupting the communication between infected endpoints and attackers	
45	The solution must provide visibility into application health history along with health status history of network applications.	
46	The solution must support custom script upload via Centralize manager so that same script can be used on multiple NGFW and it should support using FQDN to connect between the Firewall and management server & Log Server.	
47	The solution must support Multi-Layer Traffic Normalization/Full-Stream Deep Inspection, Anti-Evasion Defense, Dynamic Context Detection, Protocol-Specific Traffic Handling/Inspection, Granular Decryption of SSL/TLS Traffic (both TLS 1.2 and 1.3), Vulnerability Exploit Detection, Custom Fingerprinting, Reconnaissance, Anti- Botnet, Correlation, Traffic Recording, DoS/DDoS Protection, Blocking Methods, Automatic Updates	

48	The management platform must be a dedicated OEM appliance/software/vm running on server and should be capable of managing all the firewalls from day 1	
49	Solution must support File Filtering via Policy for minimum 200 file types in 15 categories and also support file Reputation checking & blocking for file with Malware reputation	
50	The solution should come with a web-based administration interface in the dedicated centralized manager and must be able to define the custom roles in addition to predefined roles (e.g., Owner, Viewer, Operator, Editor, Super User) to control permissions flexibly and accurately. Solution must support Documented API enabling easy third-party product and service integration Using REST architecture where data can be XML or JSON coded.	
51	The Firewall appliance must have the ability to support high availability of different model /appliances and versions within the same HA cluster negatively will be preferred.	
52	The NGFW should be proposed with all the subscription licenses for NGFW, NGIPS, Anti-Malware, URL Filtering, DNS sinkholing, DNS Proxy features as mentioned above from the date of Go-live.	
53	Solution should provide on Prem APT with Advanced threat protection capabilities for all the major Operating system like Windows, Linux, and Android & solution must deliver low level visibility to file execution activities by looking at custom OS Kernals	
54	Solution must have several static security scans including advanced signature analysis, post which files are detonated by to offer low level visibility to file, network and in memory operations of files as they execute and once the scan is completed, solution must provide a Threat Score and detailed File Threat Analysis, including a Mitre Attack matrix of the suspicious activity.	
55	Sandboxing scan must provide an advanced Threat report, including Mitre Attack insights for threat hunters, analysis of network vulnerabilities and security hardening and must support detection of zip bomb hidden threats and must we go down upto 8 layers when it comes to nested zips.	
56	Sandboxing solution must provide ability to detect and report on Ranswomware notes and must detect in memory operations for malicious behavior.	
57	The sandboxing solution must be able to analyze various threats, including malware, exploit kits, ransomware, and zero-day vulnerabilities and solution must be scalable to accommodate increasing threat analysis needs	
58	Solution must support for atleast 500 files per hours and solution must be scalable to process more files by increasing the compute, however no additional should be required.	